REMARKS

Claims 1, 2 and 12 are amended to be in better compliance with 35 USC 112, second paragraph. Specifically, claim 1 is amended to remove some language awkwardness by shifting a clause to an earlier spot in the sentence. Claim 2 is amended to remove an error in referring to the result of the step as having a subsequent action taken. Ditto for claim 12. It is an intermediate result – the decrypted identifier – that is acted on by the step of comparing. Ditto for claim 12.

Claims 1-2, 4-12, 14-22, and 29-31 were rejected under 35 USC 103 as being unpatentable over Williams US Patent 6,304,973 in view of Ichikawa et al, US Patent 6.307,837. Applicant respectfully traverses.

With respect to claims 1, 11, and 21, the Examiner states that Williams teaches a method for filtering packets using a policy. That, basically, merely states that the intended goal of Williams and of the subject claims is roughly the same. Of course, it is the *steps taken to reach the goal*, i.e., the method steps themselves, that matter.

Williams teaches the notion of identifying and verifying a user of a terminal. Once the user is identified, packets are communicated with the data encrypted by wmeans of exchanged keys (see col. 8, lines 38-43). This authentication process is not related to filtering of packets and, correctly, the Examiner does not focus on this aspect of the Williams reference. Rather, the Examiner focuses on the notion of employing a policy in connection with filtering a packets. Indeed, the passage cited by the Examiner in support of his assertion of what Williams teaches (col. 15, line 66 - col. 16, line 25) teaches that there is "rudimentary port filtering based on TCP and UDP ports."

It is noted that the TCP and UDP ports are *process* identifiers -- not hardware/computer/hosts identifiers (see col. 16, lines 5-8), and the policy related to this filtering specifies which source *processes* can communicate with which *destination* processes.

The Examiner continues by admitting that "Williams fails to specifically teach verifying the first device (source address) that is included in the transferred packet" but that "Ichikawa et al teaches a method for packet transferring at the start of communication using a gateway to authenticate the identity of the remote terminal...." The Examiner is not explicit as to how the two references are combined, but as best

understood, the Examiner suggests that the Williams system be modified to add to the notion of terminal authentication in accord with the teaching of Ichikawa et al. If that were the case, in addition to the user identification, the remote host would, presumably, obtain the source address of the packet, and apply the Ichikawa et al authentication process to determine whether the terminal is one that is permitted to partake of the requested communication, based on some policy.

Initially, there is the issue of motivations. First, once the user is authenticated there is no motivation for authenticating the terminal. Williams apparently determined that an authenticated user should be served regardless of which terminal is used. Second, even if there was any motivation for authenticating both the user and the terminal, there is no motivation for employing a policy as to which terminal is permitted and which is not. Hence, since it is believed that there is no motivation for modifying the Williams system as suggested by the Examiner, it follows that claims 1, 11, and 21 are not obvious in view of the Williams and Ichikawa et al references.

Furthermore, even if the Williams system were to be modified as suggested by the Examiner, the received packet's source address would be taken from the received packet – which arrives with the identifier (source address) in the clear. Applicant's claims, in contradistinction, specify that the received packet contains an encrypted identifier. Therefore, the combination of references as suggested by the Examiner would fail to meet an explicit limitation of claims 1, 11, and 21, which makes the claims allowable over the cited references. Additionally, it is noted that the claims also include the explicit limitation that the remainder of the packet is in the clear, and that is not true with either of the cited references. See Williams col. 8, lines 39-43, and Ichikawa et al col. 8, lines 9-13. That also constitutes a patentable difference between claims 1, 11, and 21 and the combination of the cite references.

Therefore, because of at least two lack-of-motivation reasons, and at least two explicit limitations reasons, it is respectfully submitted that claims 1, 11 and 21 are not obvious in view of the Williams and Ichikawa et al references.

The remaining claims depend on claims 1, 11, or 21 and, therefore, are believed to not be obvious in view of the cited combination of references.

Additionally, at least some of the dependent claims contain limitations that make the claims not obvious in view of the cited combination of references.

For example, as for amended claims 2 and 12, the Williams system as modified according to Ichikawa et al to include a "first device" authentication does not include decrypting the device identifier and, therefore, the first limitation of the claim is not met. The second limitation is also not met because, as stated above, there is no motivation for including the policy considerations of the TCP and UDP process considerations into the consideration of device authentication – especially since no such policy considerations have been applied to user authentication. Put simply, if there is no need to consider *policy* in connection with a user – but only to determine whether the user is *bona fide*, there is absolutely no reason to consider *policy* in connection with identification of the device that the user is using.

As for claims 6 and 16, they specify sending a message to a third device. It is noted that in the context of applicant's claims, the first device corresponds to the Williams terminal that the user is using, and the second terminal corresponds to the host to which the Williams security device is connected. Therefore, the question must be asked: what is the "third device" to which a notice is sent that the submitted identifier is not authentic? The Examiner cited Ichikawa col. 18, lines 25-28, but this passage does not teach sending anything to anywhere when authentication fails. The only thing it does teach is that when authentication fails, the packet is discarded. It is noted that the Examiner has not identified such a "third device." Hence, applicant respectfully submits that claims 6 and 16 include a limitation that is not found in the combination of Williams and Ichikawa et al. Claim 16

Claim 8 and 18 specify that a received packet is encrypted in such a way that when a first step of decryption is taken, what remains is a packet that includes an encrypted device identifier (a "two level" encryption). The Examiner cites Ichikawa et al col. 9, lines 44-64, but the cited passage describes merely a "one level" of encryption. The packets of Ichikawa, when decrypted, do not result in packets that contain an encrypted device identifier. Therefore, it

is respectfully submitted that claims 8 and 18 are not obvious in view of the Williams and Ichikawa et al combination of references.

In light of the above amendments and remarks, applicant respectfully submits that all of the Examiner's rejections have been overcome. Reconsideration and allowance are respectfully solicited.

Respectfully,
Steven M. Bellovin

Dated: 6/11/04

By _____
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net